



Министерство науки и высшего образования Российской Федерации  
Федеральное государственное бюджетное образовательное учреждение  
высшего образования  
«Московский государственный технический университет  
имени Н.Э. Баумана  
(национальный исследовательский университет)»  
(МГТУ им. Н.Э. Баумана)

---

ФАКУЛЬТЕТ «Информатика и системы управления»

---

КАФЕДРА «Программное обеспечение ЭВМ и информационные технологии»

---

ДИСЦИПЛИНА «Защита информации»

---

ОТЧЁТ  
*К ЛАБОРАТОРНОЙ РАБОТЕ 1*  
*НА ТЕМУ:*

«Энигма»

Студент группы ИУ7-72Б

\_\_\_\_\_  
(Подпись, дата)

Комаров Н.С.

\_\_\_\_\_  
(Фамилия И.О.)

Преподаватель

\_\_\_\_\_  
(Подпись, дата)

Чиж И.С.

\_\_\_\_\_  
(Фамилия И.О.)

2023 г.

## 1 Введение

**Цель** лабораторной работы — разработать программу шифровальной машины «Энигма». Составлен ряд **задач**.

- 1) Ознакомиться с устройством работы «Энигмы».
- 2) На основе «Энигмы» разработать алгоритм, позволяющий шифровать бинарные файлы.
- 3) Разработать программу, реализующую данный алгоритм.
- 4) Провести тестирование разработанной программы.

## 2 Теория

«Энигма» состоит из трёх основных компонентов: набора роторов, рефлексора и коммутационной панели, а также клавиатуры. При нажатии клавиши посылается сигнал, который проходит через коммутационную панель, потом через все роторы, отражается в рефлексоре и возвращается аналогичным путём, подсвечивая одну из лампочек-букв.

Коммутационная панель представляет собой набор гнезд под каждую букву алфавита. В комплекте с «Энигмой» идёт набор проводов, позволяющий соединить любую пару таких «слотов» между собой, таким образом произведя замену этих символов друг на друга.

Роторы представляют собой диски, с наборами контактов с обеих сторон. Контакты одной стороны произвольным образом связаны с контактами другой. После нажатия клавиши на клавиатуре, первый ротор он совершает вращение на одну позицию. Когда любой из роторов совершает полный оборот, следующий ротор совершает одно вращение.

Рефлексор попарно соединяет все буквы алфавита, и, получив сигнал, «разворачивает» его, таким образом подсвечивая пользователю зашифрованную букву.

### 3 Разработка программы

Для реализации программы был выбран язык программирования C++. Разработанная программа поддерживает три режима работы:

- 1) работа с текстовыми файлами в кодировке Windows1251, содержащими текст только на русском языке;
- 2) работа с текстовыми файлами в кодировке Windows1251, содержащими текст только на английском языке;
- 3) работа с бинарными файлами.

Запуск программы осуществляется через командную строку, в аргументах необходимо указать имена входного и выходного файлов. Пример: `./enigma-console.exe input output`

#### 3.1 Тестирование

Тестирование разработанной программы проводилось методологией «чёрного ящика». В таблице 1 приведены примеры тестов.

Таблица 1 — Тестирование

Входной файл	Результат	Режим работы
пустой файл	пустой файл	все
Hello world	MGDZT URFGJ	eng
MGDZT URFGJ	HELLO WORLD	eng
Привет мирЪ	СХАЛЛУ ЫЗСУ	ru
СХАЛЛУ ЫЗСУ	ПРИВЕТ МИРЪ	ru
hello, world! Привет, мирЪ	<что-то на бинарном>	bin
<что-то на бинарном>	hello, world! Привет, мирЪ	bin
<zip архив>	<bin>	bin
<bin>	<zip архив>	bin